Amendments to the Claims

1. (Currently Amended) A method comprising:

decrypting encrypted data that resides on one or more memory surfaces ~~associated with~~ established on a video card, said act of decrypting being performed under the influence of a cryptographic processor that resides on the video card, said act of decrypting taking place only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card and is separate from the cryptographic processor;

performing an operation on the decrypted data using the GPU to provide resultant data;

re-encrypting, under the influence of the cryptographic processor, the resultant data; and

writing the encrypted resultant data to a memory surface associated with the video card, wherein:

a trusted software component establishes the one or more memory surfaces on the video card and negotiates one or more keys with the cryptographic processor to associate each of the one or more memory surfaces with at least one unique key; and

the cryptographic processor distributes the negotiated one or more keys to cryptographic hardware of the GPU which uses the keys to perform the acts of decrypting and re-encrypting;

at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis ~~and being performed by encryption/decryption hardware integrated with the GPU~~.

2. **(Canceled)**

3. **(Original)** The method of claim 1, wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers.

4. **(Original)** The method of claim 1, wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page.

5. **(Original)** The method of claim 1, wherein the act of decrypting and re-encrypting take place on a pixel-by-pixel basis.

6. **(Original)** The method of claim 1, wherein the cryptographic processor comprises a hardware component mounted on the video card.

7. **(Original)** The method of claim 1, wherein the cryptographic processor comprises an integrated circuit chip mounted on the video card.

8. **(Original)** The method of claim 1, wherein the cryptographic processor comprises a trusted component.

9. **(Original)** The method of claim 1 further comprising receiving pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the one or more memory surfaces.

10. **(Original)** The method of claim 1 further comprising receiving pre-swizzled encrypted data that has been pre-swizzled by trusted software, and writing the pre-swizzled encrypted data to the one or more memory surfaces.

11. **(Original)** The method of claim 1, wherein the act of decrypting comprises caching decrypted pages in a local page pool cache to avoid multiple decryptions if a same page is needed.

12. **(Currently Amended)** A method comprising:

decrypting encrypted data that resides on one or more memory surfaces associated with a video card, said act of decrypting being performed under the influence of a cryptographic processor that resides on the video card, said act of decrypting taking place only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card;

performing an operation on the decrypted data using the GPU to provide resultant data;

re-encrypting, under the influence of the cryptographic processor, the resultant data; and

writing the encrypted resultant data to a memory surface associated with the video card, wherein:

a trusted software component establishes the one or more memory surfaces on the video card and negotiates one or more keys with a cryptographic processor provided on the video card separate from the GPU to associate each of the one or more memory surfaces with at least one unique key; and

the cryptographic processor distributes the negotiated one or more keys to cryptographic hardware of the GPU which uses the keys to perform said acts of decrypting and re-encrypting;

said acts of decrypting and re-encrypting taking place on a per cache page basis ~~and being performed using encryptors and decryptors of the GPU~~.

13. (Original) The method of claim 12, wherein the memory surfaces reside on the video card.

14. (Original) The method of claim 12, wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers.

15. (Original) The method of claim 12, wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page.

16. (Original) The method of claim 12, wherein the act of decrypting and re-encrypting take place on a pixel-by-pixel basis.

17. (Original) The method of claim 12, wherein the cryptographic processor comprises a hardware component mounted on the video card.

18. (Original) The method of claim 12, wherein the cryptographic processor comprises an integrated circuit chip mounted on the video card.

19. (Original) The method of claim 12, wherein the cryptographic processor comprises a trusted component.

20. (Original) The method of claim 12 further comprising receiving pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the one or more memory surfaces.

21. (Original) The method of claim 12 further comprising receiving pre-swizzled encrypted data that has been pre-swizzled by trusted software, and writing the pre-swizzled encrypted data to the one or more memory surfaces.

22. (Original) The method of claim 12, wherein the act of decrypting comprises caching decrypted pages in a local page pool cache to avoid multiple decryptions if a same page is needed.

23. (Currently Amended) A method comprising:

decrypting encrypted data that resides on one or more memory surfaces of a video card memory, said act of decrypting taking place only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card;

performing an operation on the decrypted data using the GPU to provide resultant data;

re-encrypting the resultant data; and

writing the encrypted resultant data to a video card memory surface associated with the video card, wherein:

a trusted software component establishes the one or more memory surfaces on the video card and negotiates one or more keys with a cryptographic processor provided on the video card separate from the GPU to associate each of the one or more memory surfaces with at least one unique key; and the cryptographic processor distributes the negotiated one or more keys to cryptographic hardware of the GPU which uses the keys to perform said acts of decrypting and re-encrypting;

at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis ~~and being performed by encryption/decryption hardware integrated with the GPU~~.

24. (Original) The method of claim 23, wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers.

25. (Original) The method of claim 23, wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page.

26. (Original) The method of claim 23, wherein the acts of decrypting and re-encrypting take place on a pixel-by-pixel basis.

27. (Canceled)

28. (Original) The method of claim 23 further comprising receiving pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the one or more memory surfaces.

29. **(Original)** The method of claim 23 further comprising receiving pre-swizzled encrypted data that has been pre-swizzled by trusted software, and writing the pre-swizzled encrypted data to the one or more memory surfaces.

30. **(Original)** The method of claim 23, wherein the act of decrypting comprises caching decrypted pages in a local page pool cache to avoid multiple decryptions if a same page is needed.

31. **(Currently Amended)** A method comprising:

decrypting encrypted data that resides on one or more memory surfaces of a video card memory, said act of decrypting taking place only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card;

performing an operation on the decrypted data using the GPU to provide resultant data;

re-encrypting the resultant data; and

writing the encrypted resultant data to a video card memory surface associated with the video card, wherein:

a trusted software component establishes the one or more memory surfaces on the video card and negotiates one or more keys with a cryptographic processor provided on the video card separate from the GPU to associate each of the one or more memory surfaces with at least one unique key; and the cryptographic processor distributes the negotiated one or more keys to cryptographic hardware of the GPU which uses the keys to perform said acts of decrypting and re-encrypting;

said acts of decrypting and re-encrypting taking place on a per cache page basis ~~and being performed by encryption/decryption hardware integrated with the GPU~~.

32. (Original) The method of claim 31, wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers.

33. (Original) The method of claim 31, wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page.

34. (Original) The method of claim 31, wherein the acts of decrypting and re-encrypting take place on a pixel-by-pixel basis.

35. (Canceled)

36. (Original) The method of claim 31 further comprising receiving pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the one or more memory surfaces.

37. (Original) The method of claim 31 further comprising receiving pre-swizzled encrypted data that has been pre-swizzled by trusted software, and writing the pre-swizzled encrypted data to the one or more memory surfaces.

38. (Original) The method of claim 31, wherein the act of decrypting comprises caching decrypted pages in a local page pool cache to avoid multiple decryptions if a same page is needed.

39. (Currently Amended) A system comprising:

means residing on a graphics processor unit (GPU) for decrypting, on a per cache page basis, encrypted data that resides on one or more memory surfaces of a video card memory only when an operation is to be performed on the data by the graphics processor unit (GPU) that resides on the video card;

means for performing an operation on the decrypted data to provide resultant data;

means residing on the graphics processor unit (GPU) for re-encrypting, on a per cache page basis, the resultant data; ~~and~~

means for writing the encrypted resultant data to a video card memory surface associated with the video card, and

a trusted software component to establish the one or more memory surfaces on the video card and negotiate one or more keys with the cryptographic processor such that each of the one or more memory surfaces is associated with at least one unique key;

wherein the cryptographic processor distributes the one or more keys to said means for decrypting and said means for re-encrypting to perform the decrypting and re-encrypting respectively.

40. **(Original)** The system of claim 39, wherein the means for decrypting comprises, at least in part, cryptographic hardware inside the GPU.

41. **(Original)** The system of claim 39, wherein the means for performing comprises a GPU.

42. **(Original)** The system of claim 39, wherein the means for re-encrypting comprises, at least in part, cryptographic processor hardware mounted on the video card.

43. **(Original)** The system of claim 39, wherein said means for decrypting and re-encrypting comprise one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page.

44. **(Original)** The system of claim 39 further comprising means for pooling decrypted pages to avoid multiple decryptions of a page that might be needed more than once.

45. **(Currently Amended)** A system comprising:

a video card;

a graphics processor unit (GPU) on the video card and configured to process video data that is to be rendered on a display device;

memory on the video card comprising one or more input memory surfaces configured to hold encrypted data that is to be operated upon by the GPU, and one or more output memory surfaces configured to hold encrypted resultant data that is to be rendered on the display device;

a cryptographic processor on the video card and configured to initialize cryptographic hardware of the GPU including one or more encryptors and one or more decryptors to control encryption and decryption on the video card, the cryptographic processor being configured to enable encrypted data on one or more of the input memory surfaces to be decrypted, on a per cache page basis by decryption hardware inside the GPU, in connection with an operation that is to be performed on the data by the GPU; and

a trusted software component to negotiate one or more keys with the cryptographic processor such that each of the one or more input and output memory surfaces is associated with at least one unique key

the cryptographic processor further being configured to distribute said negotiated keys to the cryptographic hardware of the GPU to enable data that has been operated upon by the GPU to be encrypted, on a per cache page basis by ~~encryption hardware inside the~~ said one or more encryptors of the GPU, to an output memory surface.

46. (Original) The system of claim 45, wherein the cryptographic processor is configured to use block ciphers to effect encryption and decryption.

47. (Original) The system of claim 45, wherein the cryptographic processor is configured to use one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page.

48. (Original) The system of claim 45, wherein the cryptographic processor comprises a hardware component mounted on the video card.

49. (Original) The system of claim 45, wherein the cryptographic processor comprises an integrated circuit chip.

50. (Original) The system of claim 45, wherein the cryptographic processor comprises a trusted component.

51. (Original) The system of claim 45, wherein the cryptographic processor is configured to set up a session key with a trusted software component.

52. (Original) A computer system embodying the system of claim 45.

53. (Currently Amended) A method comprising:

providing multiple input memory surfaces that are to hold encrypted data that is to be processed by a graphics processor unit (GPU) on a video card;

associating, with each input memory surface, a decryptor of the GPU that is uniquely configured so as to decrypt the encrypted data that is held by the associated input memory surface;

decrypting, with at least one associated decryptor, encrypted data that resides on at least one respective input memory surface;

performing an operation on the decrypted data using the GPU to provide resultant data;

re-encrypting the resultant data; and

writing the encrypted resultant data to an output memory surface associated with the video card;

wherein the video card includes a cryptographic processor as a distinct component that is configured to:

negotiate one or more cryptographic keys with a trusted software component; and

initialize said decryptor of the GPU to perform said act of decrypting,

at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis ~~and being performed by encryption/decryption hardware integrated with the GPU~~.

54. (Original) The method of claim 53, wherein the act of providing the multiple input memory surfaces comprises providing at least one input memory surface on the video card.

55. (Currently Amended) The method of claim 53, wherein the act of re-encrypting comprises using an encryptor of the GPU that is uniquely associated with the output memory surface to re-encrypt the resultant data , and the cryptographic processor is further configured to initialize said encryptor of the GPU to perform said act of re-encrypting.

56. (Previously Presented) The method of claim 53, wherein the act of re-encrypting comprises using an encryptor of the GPU that is uniquely associated with the output memory surface to re-encrypt the resultant data, and wherein negotiated key indices are used to identify and regulate which keys are used in decrypt and re-encrypt operations.

57. (Original) The method of claim 53, wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers.

58. (Original) The method of claim 53, wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page.

59. (Original) The method of claim 53, wherein the acts of decrypting and re-encrypting take place on a pixel-by-pixel basis.

60. (Original) The method of claim 53, wherein the acts of decrypting and re-encrypting are performed under the influence of a cryptographic processor that resides on the video card.

61. (Original) The method of claim 60, wherein the cryptographic processor comprises an integrated circuit chip.

62. (Original) The method of claim 60, wherein the cryptographic processor comprises a trusted component.

63. (Original) The method of claim 53, wherein the act of decrypting is performed only when the GPU is to perform an operation on data that resides on a particular input memory surface.

64. (Original) The method of claim 53 further comprising restricting one or more operations that can be performed by the GPU based on whether encrypted output is available.

65. (Original) The method of claim 53 further comprising decrypting the encrypted resultant data for rendering on a display device.

66. (Original) The method of claim 53 further comprising decrypting, with a display convertor, the encrypted resultant data for rendering on a display device.

67. (Original) The method of claim 53 further comprising receiving pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the input memory surfaces.

68. (Original) The method of claim 53 further comprising receiving pre-swizzled encrypted data that has been pre-swizzled by trusted software, and writing the pre-swizzled encrypted data to the input memory surfaces.

69. (Original) The method of claim 53, wherein the act of decrypting comprises caching decrypted pages in a local page pool cache to avoid multiple decryptions if a same page is needed.

70. (Currently Amended) A method comprising:

providing multiple input memory surfaces that are to hold encrypted data that is to be processed by a graphics processor unit (GPU) on a video card;

associating, with each input memory surface, a decryptor that is uniquely configured so as to decrypt the encrypted data that is held by the associated input memory surface;

decrypting, with at least one associated decryptor, encrypted data that resides on at least one respective input memory surface;

performing an operation on the decrypted data using the GPU to provide resultant data;

re-encrypting the resultant data; and

writing the encrypted resultant data to an output memory surface associated with the video card,

wherein the video card includes a cryptographic processor as a distinct component that is configured to:

negotiate one or more cryptographic keys with a trusted software component; and

initialize said decryptor of the GPU to perform said act of decrypting

said acts of decrypting and re-encrypting taking place on a per cache page basis ~~and being performed by encryption/decryption hardware integrated with the GPU~~.

71. **(Original)** The method of claim 70, wherein the act of providing the multiple input memory surfaces comprises providing at least one input memory surface on the video card.

72. **(Original)** The method of claim 70, wherein the act of re-encrypting comprises using an encryptor that is uniquely associated with the output memory surface to re-encrypt the resultant data.

73. **(Original)** The method of claim 70, wherein the act of re-encrypting comprises using an encryptor that is uniquely associated with the output memory surface to re-encrypt the resultant data, and wherein negotiated key indices are used to identify and regulate which keys are used in decrypt and re-encrypt operations.

74. **(Original)** The method of claim 70, wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers.

75. **(Original)** The method of claim 70, wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page.

76. **(Original)** The method of claim 70, wherein the acts of decrypting and re-encrypting take place on a pixel-by-pixel basis.

77. (Original) The method of claim 70, wherein the acts of decrypting and re-encrypting are performed under the influence of a cryptographic processor that resides on the video card.

78. (Original) The method of claim 77, wherein the cryptographic processor comprises an integrated circuit chip.

79. (Original) The method of claim 77, wherein the cryptographic processor comprises a trusted component.

80. (Original) The method of claim 70, wherein the act of decrypting is performed only when the GPU is to perform an operation on data that resides on a particular input memory surface.

81. (Original) The method of claim 70 further comprising restricting one or more operations that can be performed by the GPU based on whether encrypted output is available.

82. (Original) The method of claim 70 further comprising decrypting the encrypted resultant data for rendering on a display device.

83. **(Original)** The method of claim 70 further comprising decrypting, with a display convertor, the encrypted resultant data for rendering on a display device.

84. **(Original)** The method of claim 70 further comprising receiving pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the input memory surfaces.

85. **(Original)** The method of claim 70 further comprising receiving pre-swizzled encrypted data that has been pre-swizzled by trusted software, and writing the pre-swizzled encrypted data to the input memory surfaces.

86. **(Original)** The method of claim 70, wherein the act of decrypting comprises caching decrypted pages in a local page pool cache to avoid multiple decryptions if a same page is needed.

87. **(Currently Amended)** A system comprising:

a video card;

a graphics processor unit (GPU) on the video card and configured to process video data that is to be rendered on a display device;

memory on the video card comprising one or more input memory surfaces configured to hold encrypted data that is to be operated upon by the GPU, and one or more output memory surfaces configured to hold encrypted resultant data that is to be rendered on the display device;

a cryptographic processor on the video card and configured to control encryption and decryption on the video card, the cryptographic processor comprising a key manager for managing keys that can be utilized for encrypting and decrypting data on the video card, ~~the GPU comprising encryption and decryption hardware operable under the influence of the cryptographic processor to perform cryptographic operations;~~ said managing keys including:

negotiating the keys with a trusted software component such that each individual input memory surface has ~~having~~ its own unique associated key for decrypting encrypted data held thereon;

~~the cryptographic processor being configured~~ distributing corresponding keys to the GPU to enable encrypted data on one or more of the input memory surfaces to be decrypted by the GPU on a per cache page basis so that the decrypted data can be operated upon by the GPU; and

~~the cryptographic processor further being configured~~ distributing corresponding keys to the GPU to enable data that has been operated upon by the GPU to be encrypted on a per cache page basis to an output memory surface.

88. **(Original)** The system of claim 87, wherein the cryptographic processor is configured to control encryption and decryption using block ciphers.

89. **(Original)** The system of claim 87, wherein encryption and decryption takes place on a pixel-by-pixel basis.

90. **(Original)** The system of claim 87, wherein encrypted data held on an input memory surface is decrypted only when it is to be operated upon by the GPU.

91. **(Original)** The system of claim 87, wherein the cryptographic processor comprises an integrated circuit chip.

92. **(Original)** The system of claim 87, wherein the cryptographic processor comprises a trusted component.

93. **(Original)** The system of claim 87, wherein the cryptographic processor is configured to set up a session key with a trusted software component.

94. **(Original)** A computer system embodying the system of claim 87.